

计算机网络环境下区块链数据共享的可信机制研究

张 瑞 郭庆平

郑州电子商务职业学院 河南郑州 450000

摘 要: 随着信息技术的迅速发展, 计算机网络环境下的数据共享需求日益增长, 数据可信性和安全性成为亟需解决的重要问题。区块链技术因其去中心化、防篡改和可追溯等特性, 在数据共享领域展现出巨大的应用潜力。本研究聚焦于区块链环境中数据共享的可信机制, 分析了现有网络数据共享模式存在的安全隐患及信任缺失等问题。在深入剖析区块链技术优势的基础上, 提出了一种基于多节点协作与智能合约相结合的可信数据共享机制, 通过多方验证与自动执行实现数据传输过程的可控性与透明化。结果显示, 该机制能够有效提升数据共享过程中的信任度, 降低信息泄露风险, 增强数据溯源能力。研究进一步指出, 区块链数据共享模式有助于推动各行业间的信息互联互通, 优化跨部门数据协作效率, 对建立健全的网络信任体系具有重要现实意义。

关键词: 区块链技术; 数据共享; 可信机制; 智能合约; 网络安全

引言

随着社会数字化转型进程的加快, 计算机网络环境下数据共享需求呈现爆发式增长。海量数据在不同主体与系统间传输与流通, 数据的可信性与安全性问题尤为突出。目前, 传统数据共享模式普遍依赖中心化服务器, 存在单点故障、数据篡改及隐私泄露等诸多隐患, 难以应对分布式环境下风险与挑战。根据《中国互联网发展状况统计报告》(www.cnnic.net.cn), 我国网络用户总量及数据交互频次持续攀升, 数据共享的安全保障问题日趋迫切。近年来, 区块链技术凭借去中心化、防篡改、全程可追溯等特性, 在数据共享领域展现出变革潜力。国内外学者针对区块链应用做了大量探索, 如基于共识机制优化数据流转、防范恶意节点攻击等, 但在多节点协同及智能合约自动执行保障数据可信共享方面仍存在不足。因此, 深入研究并构建适应复杂计算机网络环境的区块链数据共享可信机制, 既有助于提升数据传输的

安全与透明性, 又为健全网络信任体系奠定基础。本文旨在提出并验证一种基于多节点协作与智能合约结合的区块链数据共享可信机制, 以期为数字社会发展提供可靠保障。

一、区块链技术在网络数据共享中的应用背景

1. 计算机网络数据共享的现状与挑战

随着互联网技术的普及与发展, 计算机网络环境中的数据共享已成为推动信息传播与知识交流的重要手段^[1]。现阶段的网络数据共享面临诸多挑战。数据共享的安全性问题日趋严重, 不同组织和用户对网络信任体系的质疑导致信任缺失。传统中心化的数据管理模式存在显著弊端, 容易出现单点故障, 使数据篡改与信息泄露风险增加。网络攻击和恶意行为者通过拦截、篡改数据进一步削弱了数据的完整性和可信性, 这对数据所有者和使用者造成了严重影响, 阻碍了数据的高效流通与共享。针对这些问题, 探索创新的数据共享机制以满足安全和可信的双重需求已势在必行。区块链技术因其独特的特性为解决这些挑战提供了新的思路^[2]。

2. 区块链技术的核心特性

区块链技术以其去中心化、防篡改和可追溯性等核心特性, 成为现代数据共享机制中备受关注的技术方案。去中心化使得数据存储不依赖单一中心节点, 而通过全网节点共同维护, 增强了信息的可靠性及一致性; 防篡改特性则来源于其密码学机制, 确保数据在记录后无法

作者简介:

- 张瑞, 出生年: 1998年1月, 性别: 女, 民族: 汉, 籍贯: 河南省周口市, 单位: 郑州电子商务职业学院, 职称: 助教, 学位: 学士, 主要研究方向: 区块链技术。
- 郭庆平, 出生年月: 1987年10月, 性别: 男, 民族: 汉, 籍贯: 河南省周口市, 单位: 郑州电子商务职业学院, 职称: 实验师, 学位: 硕士, 主要研究方向: 信息管理。

被修改，提升数据完整性；可追溯性通过链上的数据记录实现透明化的数据流向查询，方便溯源审计。这些特性结合起来，有助于构建一个安全可信的网络数据共享环境，改善信任基础，提升协作效率。

3. 数据共享对可信机制的需求

数据共享的过程需确保信息的完整性、真实性和可追溯性，这对于建立稳固的网络信任机制尤为重要^[3]。在传统环境中，数据传输常面临篡改与泄露风险，从而导致信任缺失。可信机制的需求愈发紧迫，旨在保障数据在共享过程中的不可篡改和真实验证。区块链技术凭借其去中心化和智能合约功能，可有效克服现有系统中的信任缺陷，确保数据在多方之间的透明流动，降低信息泄露的可能性，有助于建立健全的数据安全体系。

二、传统数据共享模式的安全隐患

1. 网络信任体系的缺陷

网络信任体系在传统数据共享模式中存在显著缺陷，直接影响了数据流通的可靠性与安全性。传统模式通常依赖于中心化的信任机构或中介来确保数据安全，这种依赖模式导致了一系列问题，其中包括单点故障风险和信任单元的过度集中。中心化信任机制易受攻击和操控，从而削弱了整体系统的安全性。过度依赖第三方信任机构可能导致信任传递过程中的信息孤岛现象，限制了信息的广泛共享和有效利用。在跨部门或跨行业数据共享中，传统信任体系难以为数据使用者和提供者之间建立健全的信任关系，造成数据透明度和可信度的不足。这些缺陷在当今信息技术快速发展的环境下被愈发凸显，亟需改进。区块链技术的去中心化属性提供了优化信任体系的新思路。

2. 数据篡改与信息泄露风险

在传统的共享模式中，数据篡改与信息泄露的风险较为突出。因集中式存储与管理模式，权限集中于单一或少数管理者，增加了内部或外部攻击者利用系统漏洞篡改数据的可能性。缺乏有效的追溯机制使篡改行为难以被及时发现与修复。信息在传输过程中依赖中心服务器，易受拦截与窃取。数据加密措施虽可减少部分信息暴露，但仍无法完全防御高级别黑客攻击。信息泄露事件的频发不仅损害了数据所有者的合法权益，也严重削弱了用户对系统的信任和依赖。

3. 信任缺失对数据流通的影响

信任缺失对数据流通的影响显著且深远。在传统数据共享模式中，信任机制通常依赖于中心化的第三方实

体，其透明度及可靠性常受到质疑。信息发送方无法完全确信接收方的身份及数据接收意图，而接收方也难以保证数据的完整性与真实性。这种互信障碍导致数据流通效率低下，广泛增加了数据篡改与欺诈行为的风险，限制了各方之间信息共享的积极性与合作意愿，妨碍了网络环境中数据价值的最大化利用与创新发展。

三、区块链环境下可信数据共享机制构建

1. 多节点协作的信任基础

在区块链环境下构建可信数据共享机制中，多节点协作所形成的信任基础至关重要。多节点协作意味着区块链网络中的每个节点都参与数据验证和共识达成，从而确保数据的完整性与真实性。这种机制通过分布式账本技术保障数据不被单点控制，实现了去中心化的强健信任结构^[4]。节点间的交互采用加密算法维护数据传输的安全性，抵御潜在的网络攻击。节点之间的数据同步和更新过程基于共识算法，能够有效避免因人为或系统错误导致的信任缺失问题。这种信任基础促进了信息的可信流通，为跨领域的数据共享奠定了稳固的安全保障，进而推动各行业间的数据协作与创新发展。多节点协作不仅是技术层面的突破，更是构建可信数据共享生态系统的重要环节。区块链技术通过这种信任基础，有效提升了数据透明度和可靠性，将成为网络信任体系中不可或缺的组成部分。

2. 智能合约实现数据共享的透明性

在区块链环境下，智能合约是实现数据共享透明化的重要工具。智能合约通过其自我执行的特点，确保数据共享协议在预设条件下自动运作，减少人为干预和操作错误的可能性。合约条件的公开性和可验证性，赋予参与者更高的透明度和信任感，对交易全过程的每个步骤进行验证和记录，保证信息的真实与不可篡改。这种机制大幅降低数据泄露风险，促进不同主体间更顺畅的数据交互，实现数据共享过程的高透明度和可靠性。

3. 数据溯源与风险防控措施

在区块链环境下，实现数据溯源与风险防控至关重要。通过区块链独特的分布式账本结构，可对每个数据操作进行精确记录，确保数据来源可追踪。智能合约的自动执行性保障了数据流程的透明和不易篡改性，有效降低潜在风险。建立节点间的信任机制，在共享过程中对数据访问权限与异常行为进行实时监控，以及时识别和规避安全隐患，进一步提升数据传输的可靠性与稳健性。

四、区块链数据共享机制的行业应用价值

1. 行业间数据协作效率提升

区块链数据共享机制能够显著提升行业间的数据协作效率。这种机制支持多方协同，通过去中心化的网络结构和智能合约技术，实现数据共享的快速、透明和安全。在金融行业，区块链技术促进跨机构间数据交互的自动化处理，减少了人工干预和信息不对称，降低了交易成本^[5]。在供应链管理领域，区块链赋能下的实时数据共享提高了各方的响应速度，优化了库存管理和配送效率。在医疗行业，区块链技术促进了患者信息的安全共享和医疗资源的精准匹配，有助于加快诊疗过程。总体而言，通过减少信任壁垒与简化协作流程，区块链技术在促进行业间数据交换的效率与可靠性方面展现出强大的应用优势。

2. 网络安全体系的优化作用

区块链数据共享机制在优化网络安全体系方面展现出显著作用。通过去中心化的网络结构，区块链有效减少了单点故障的风险，增强了系统的稳定性。智能合约的使用确保了数据共享过程中的自动化管理与执行，降低了人为干预带来的安全隐患。区块链的防篡改特性提供了高度健全的数据完整性保障，确保传输和存储过程中数据的不可更改性。多节点协作则加强了多方验证的平台信任度，提高了网络环境中数据交换的安全性。这些特性共同促进了更加安全、可靠的数据共享网络的形成，推动了网络安全体系的进一步完善。

3. 信息互通与可信生态的构建

区块链数据共享机制在信息互通与可信生态构建方面发挥着关键作用。通过去中心化的架构，各行业之间能够实现更高效的数据交换，减少信息孤岛现象。智能合约的自动执行特性确保了数据共享过程的透明和可信，从而建立行业间的信任基础。数据透明性和溯源能力进一步强化了网络信任体系的稳定性，为跨行业间长期合

作提供保障。上述功能提升了信息流通的效率和安全性，促进了一个更加可信、互联互通的生态系统的发展，有助于解决信息孤立和信任缺失的挑战。

结束语

本研究针对计算机网络环境下数据共享过程中面临的信任及安全问题，深入分析了现有模式的局限性，提出了基于多节点协作与智能合约相结合的区块链可信数据共享机制。实验结果验证了所提机制在提升数据共享信任度、降低信息泄露风险及强化数据溯源方面的有效性，为优化跨部门数据协作与推动行业间信息互联互通提供了可行方案。尽管如此，目前机制在面对高并发场景、节点间数据一致性及智能合约复杂业务适应性方面仍存在一定的技术挑战。此外，区块链存储扩展性和隐私保护策略尚待进一步提升。未来研究可聚焦于区块链性能优化、智能合约安全性增强、隐私计算与分布式数据管理等方向，探索更为高效、可扩展且具备更强隐私保护的数据共享机制，为建设完善的网络信任体系和推动数据要素流通提供坚实支撑。

参考文献

- [1] 沈淑涛, 高飞. 基于区块链技术的可信光网络数据库匿名共享方法[J]. 现代电子技术, 2021, 44(21): 74-77.
- [2] 程力. 区块链技术在计算机网络安全中的应用[J]. 数字技术与应用, 2022, 40(09): 240-242.
- [3] 朱志强. 基于区块链的档案数据共享可信度机制构建[J]. 黑龙江档案, 2020, (04): 79-79.
- [4] 陈岸青, 肖郑海, 潘鑫宇. 基于数据可信共享的区块链安全技术分析[J]. 电子技术(上海), 2023, 52(01): 280-281.
- [5] 朱勇. 基于区块链的智能安防社区可信数据共享方法[J]. 自动化与仪器仪表, 2022, (08): 50-53.